

FASSE PATENT ATTORNEYS, P.A.

58-G MAIN ROAD NORTH, P.O. BOX 726  
HAMPDEN, MAINE 04444-0726 U.S.A.

TELEPHONE: 207-862-4671  
TELEFAX: 207-862-4681

WALTER F. FASSE

WOLFGANG G. FASSE  
Of Counsel

76  
#6  
12/1/03

DOCKET NO.: 4286

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN THE MATTER OF THE APPLICATION FOR PATENT

OF: Werner BLATZ

| Art Unit: 2631

SERIAL NO.: 10/071,929

| Confirmation No.: 9845

FILED: February 6, 2002

FOR: Detecting Redirection During  
Data Transmission

ASSISTANT COMMISSIONER FOR PATENTS

WASHINGTON, D.C. 20231

October 31, 2002

PRIORITY DOCUMENT TRANSMITTAL

Dear Sir:

Applicant is enclosing Priority Document No.: 101 06 736.4, filed in the Federal Republic of Germany on February 14, 2001. The priority of the German filing date is being claimed for the present application. Acknowledgement of the receipt of the Priority Document is respectfully requested.

Respectfully submitted,

Werner BLATZ

Applicant

WFF:ar/4286

Encls.: postcard,  
1 Priority Document  
as listed above

By

Walter F. Fasse  
Walter F. Fasse  
Patent Attorney  
Reg. No.: 36132

CERTIFICATE OF MAILING:

I hereby certify that this correspondence with all indicated enclosures is being deposited with the U. S. Postal Service with sufficient postage as first-class mail, in an envelope addressed to: Assistant Commissioner for Patents, Washington, D. C. 20231, on the date indicated below.

Anita Morse - October 31, 2002  
Name: Anita Morse - Date: October 31, 2002



**Prioritätsbescheinigung über die Einreichung  
einer Patentanmeldung**

**CERTIFIED COPY OF  
PRIORITY DOCUMENT**

**Aktenzeichen:** 101 06 736.4

**Anmeldetag:** 14. Februar 2001

**Anmelder/Inhaber:** ATMEL Germany GmbH, Heilbronn/DE

**Bezeichnung:** Verfahren zur Erkennung einer Weiterleitung bei  
einer bidirektionalen, kontaktlosen Datenübertragung

**IPC:** H 04 L, G 07 C, B 60 R

**Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der  
ursprünglichen Unterlagen dieser Patentanmeldung.**

München, den 17. April 2002  
Deutsches Patent- und Markenamt  
Der Präsident  
Im Auftrag

Dzierzon

Heilbronn, den 12.02.2001  
FTP/H-dk/dk - P303515

5

**Verfahren zur Erkennung einer Weiterleitung bei einer bidirektionalen, kontaktlosen Datenübertragung**

Die vorliegende Erfindung betrifft ein Verfahren zur Erkennung einer Weiterleitung bei einer bidirektionalen, kontaktlosen Datenübertragung, gemäß dem Oberbegriff des Patentanspruchs 1.

Systeme zur bidirektionalen kontaktlosen Datenübertragung werden vorzugsweise bei Identifikationssystemen eingesetzt. Im allgemeinen bestehen diese Systeme aus einer Basisstation und einem Transponder. Im KFZ-Bereich, einem Haupteinsatzgebiet werden diese Systeme zur Authentifizierung eingesetzt. Um eine hohe Sicherheit bei der Authentifizierung zu erreichen, wird die Kommunikationsentfernung bei dem sogenannten „passiv entry“, d.h. das Öffnen eines Fahrzeugs durch ein Ziehen am Türgriff auf wenige Meter beschränkt. Bei der Identifizierung ist es wichtig, daß die Zeit für den Authentifizierungsprozeß kurz bleibt. Im KFZ-Bereich liegt die Gesamtzeit für die Authentifizierung in der Regel zwischen 50 und 130 ms. Um eine unberechtigte Authentifizierung, beispielsweise durch eine Weiterleitung zu verhindern, werden Verfahren entwickelt, um die Manipulation zu erkennen und den Authentifizierungsprozeß gegebenenfalls abubrechen

Zur Erkennung einer Weiterleitung bei einem Authentifizierungsprozeß, ist aus der Druckschrift DE 10005503 ein erstes Verfahren bekannt, bei dem wenigstens eine charakteristische Größe der ausgesandten elektromagnetischen Welle reversibel geändert wird. Hierzu wird in einer zweiten Sende- und Empfangseinheit (Transponder), ein gegenüber dem Fragesignal beispielsweise in der Frequenz verändertes Antwortsignal, an die erste Sende- und Empfangseinheit zurückgesandt. In der ersten Sende- und Empfangseinheit (Basisstation) wird die Frequenz des Antwortsignals zurückgeändert und mit der Frequenz des ursprünglich ausgesandten Fragesignals verglichen. Liegt der ermittelte Wert innerhalb eines vorgegebenen Intervalls kann eine Weiterleitung weitestgehend ausgeschlossen werden.

Ein weiteres Verfahren zur Erkennung einer Weiterleitung bei einem Authentifizierungsprozeß ist aus der Druckschrift DE 198 27 722 bekannt. Um ein unberechtigtes Öffnen eines Kraftfahrzeugs zu verhindern, wird die Sendestärke des Fragesignals und des Antwortsignals bitweise moduliert. Die zur Modulation verwendete Maske wird mittels eines geheimen Schlüssels, der sowohl in der Basisstation als auch im Transponder bekannt ist, erzeugt. Ausgehend von der Annahme, daß bei einer Weiterleitung die Modulation der Sendestärke ausgewertet werden muß und es damit zu einer zusätzlichen Zeitverzögerung zwischen dem Aussenden des Fragesignals und des Empfangs des Antwortsignals kommt, wird eine zulässige Maximalzeit festgelegt. Ist die Zeitdifferenz zwischen Frage und Antwortsignal größer als die festgelegte Mindestzeit, wird von einer Weiterleitung ausgegangen und der Authentifizierungsprozeß abgebrochen.

Nachteil der bisherigen Verfahren ist, daß eine Weiterleitung durch die bisherigen Verfahren nicht oder nur unzureichend erschwert wird. Zwar erschwert das reversible Ändern der Frequenz das in der Regel bei einer Weiterleitung durchgeführte Umsetzen der Frequenz, der Grad der Erschwerung ist jedoch allein von der Präzision der Frequenzumsetzung innerhalb der Weiterleitungsgeräte bestimmt. Sofern eine hochpräzise Umsetzung und Rückumsetzung der Frequenz in den Weiterleitungsgeräten durchführbar ist, kann eine Authentifizierung durchgeführt werden und sich ein unberechtigter Zugang beispielsweise zu einem Kraftfahrzeug verschafft werden. Bei dem weiteren bekannten Verfahren, das die Weiterleitung mittels verschlüsselter Modulation der Sendeleistung zu erkennen versucht, ist dies bereits mit den derzeit bekannten Geräten zur Weiterleitung (Transceiver) durchführbar. So gleichen die bekannten Transceiver, die zusätzlichen Dämpfungsverluste, bedingt durch die größere Länge des Signalweges bei der Weiterleitung, mittels einer linearen Verstärkung der Signale aus, ohne daß die relative Modulation der Sendeleistung verändert wird. Da die Modulation der Sendeleistung nicht entschlüsselt werden muß, tritt der durch das Verfahren postulierte Zeitverlust nicht ein und eine Weiterleitung kann nicht erkannt werden. Beide Verfahren bieten keinen ausreichenden Schutz vor einem unberechtigten Zugang innerhalb eines Authentifizierungsprozesses.

Aufgabe der vorliegenden Erfindung ist es, ein Verfahren anzugeben, das eine Weiterleitung der Signale erkennt.

Die genannte Aufgabe wird durch die Merkmale des Patentanspruches 1 gelöst. Günstige Ausgestaltungsformen sind Gegenstand von Unteransprüchen.

Das Wesen der Erfindung besteht darin, daß bei einer bidirektionalen, kontaktlosen Datenübertragung mittels eines Vergleichs der Dämpfungscharakteristik der Übertragungsstrecke zwischen einer ersten Sende- und Empfangseinheit und einer zweiten Sende- und Emp-

fangseinheit festgestellt wird, ob eine Weiterleitung stattfindet. Hierzu wird in der zweiten Sende- und Empfangseinheit, das von der ersten Sende- und Empfangseinheit ausgesendete Fragesignal hinsichtlich seiner Amplitude vermessen. Der gemessene Amplitudenwert wird in einem Antwortsignal, vorzugsweise in codierter Form, an die erste Sende- und Empfangseinheit zurückgesandt. Ferner wird in der ersten Sende- und Empfangseinheit die Amplitude des empfangenen Antwortsignals bestimmt und mit dem zurückgesandten Wert der Amplitude verglichen und in Abhängigkeit des Vergleichs einer Weiterleitungsanzeige ein Wert zugeordnet. Liegt dabei das Ergebnis des Vergleichs der Amplitudenwerte innerhalb eines vorgegebenen Intervalls wird eine Weiterleitung ausgeschlossen.

10

Das erfindungsgemäße Verfahren basiert auf dem Prinzip, daß bei einer Kommunikation ohne Weiterleitung, die Übertragungsstrecke bezüglich ihres Dämpfungsverhaltens symmetrisch ist, d.h. sowohl der Hinweg als auch der Rückweg weisen die gleiche Dämpfungseigenschaft auf, da beide Sende- und Empfangseinheiten für das Senden und Empfangen von Signalen jeweils eine einzige Antenne benutzen. Werden die Signale von einem Weiterleitungsgerät verlängert, benutzt das Weiterleitungsgerät für das Senden und Empfangen unterschiedliche Antennen, um die zusätzliche Dämpfung, die durch das Weiterleitungsgerät verursacht wird, mittels einer Verstärkung der Signale auszugleichen. Mit den unterschiedlichen Antennen für das Senden und Empfangen des Weiterleitungsgeräts sind unterschiedlichen Kopplungsfaktoren zwischen den Antennen der Sende- und Empfangseinheiten und des Weiterleitungsgeräts verbunden, die die Symmetrie in der Übertragungsstrecke aufheben und die Amplitude des Fragesignals im Vergleich zu der Amplitude des Antwortsignals unterschiedlich stark bedämpfen.

25 In einer Weiterbildung des Verfahrens werden die Informationen über die Dämpfungseigenschaft des Signalweges, die sich aus dem gemessenen Wert der Amplitude extrahieren lassen, vor einem unberechtigtem Zugriff geschützt. Hierzu wird der digitalisierte Wert der Amplitude in verschlüsselter Form in das Antwortsignal eingebaut. Bei einem Authentifizierungsprozeß, bei dem die Berechtigung mittels Überprüfung von verschlüsselten ID-Codes geprüft wird, läßt sich der Wert der Amplitude mit dem gleichen Schlüssel codieren, mit dem auch der ID-Code der jeweiligen Sende- und Empfangseinheit vor der Übertragung verschlüsselt wird. Durch die Verschlüsselung ist eine Auswertung der Dämpfungsinformation mit vertretbaren Mitteln nicht durchführbar.

35 In einer anderen Weiterbildung des Verfahrens wird der Vergleich der Amplituden innerhalb eines vorgegebenen Zeitfensters durchgeführt und dabei geprüft, ob das Antwortsignal zeitlich unmittelbar auf das Fragesignal folgt. Damit wird verhindert, daß während der Kommunikation von der ersten Sende- und Empfangseinheit mit der zweiten Sende- und Empfangseinheit eine Ortsveränderung von einer der beiden Sende- und Empfangseinheiten die Sym-

metrie im Übertragungsweg aufhebt und mittels der resultierenden unterschiedlichen Dämpfung der Amplitude eine vermeintliche Weiterleitung angezeigt wird. Ferner wird verhindert, daß ein Weiterleitungsgerät durch eine mehrmalige Veränderung seiner Signalverstärkung versucht, die Unsymmetrie in der Dämpfungscharakteristik auszugleichen.

5

In einer anderen Weiterbildung des Verfahrens wird die Weiterleitung erkannt, in dem von der ersten Sende- und Empfangseinheit zusätzlich zu dem Vergleich der Amplituden auch ein Vergleich der Frequenz des Fragesignals mit der Frequenz des Antwortsignals durchgeführt wird. Um das Intervall für den Frequenzvergleich möglichst klein zu wählen, ist es vorteilhaft, wenn mit der Frequenz des von der ersten Sende- und Empfangseinheit ausgesendete Fragesignals in der zweiten Sende- und Empfangseinheit eine Frequenzkopplung durchgeführt wird. Hiermit läßt sich die Trägerfrequenz für eine Modulation der Daten des Antwortsignals regenerieren. Da die Frequenz des Antwortsignals und des Trägersignals identisch sind, lassen sich kleinste Abweichungen in der Trägerfrequenz feststellen. Eine Weiterleitung auf der selben Frequenz wird sehr erschwert, da das Weiterleitungsgerät durch eine Rückkopplung in seiner Funktion gestört wird. Eine Frequenzumsetzung vom Weiterleitungsgerät innerhalb der Weiterleitungsstrecke führt zu einem Frequenzversatz in der Trägerfrequenz. Liegt das Ergebnis des Frequenzvergleichs innerhalb des vorgegebenen Intervalls, wird eine Weiterleitung ausgeschlossen.

20

In einer anderen Weiterbildung des Verfahrens wird von der ersten Sende- und Empfangseinheit zusätzlich zu dem Vergleich der Amplitude und der Frequenz geprüft, ob das Träger-signal mit Ausnahme der Feldlücken während der Aussendung des Fragesignals bis zu dem Empfang des Antwortsignals, ohne Unterbrechung anliegt. Für ein Weiterleitungsgerät ist es daher sehr schwierig, die Trägerfrequenz für eine Weiterleitung umzusetzen, ohne daß dieses von der ersten Sende- und Empfangseinheit dedektiert wird. Eine Verstärkung der Signale, die die zusätzliche Dämpfung durch die Verlängerung des Signalweges ausgleicht, muß von dem Weiterleitungsgerät auf der Frequenz des Trägers erfolgen. Das Weiterleitungsgerät kann dabei die zusätzlichen Dämpfungsverluste nur insoweit ausgleichen, wie seine Signalverstärkung kleiner als der Wert der Entkopplung seiner Sende- und Empfangsantennen bleibt. Anderenfalls ist die Kreisverstärkung innerhalb des Weiterleitungsgeräts größer als eins und es entsteht eine Rückkopplung, durch die die Funktion des Weiterleitungsgeräts stark gestört wird.

30

Untersuchungen der Anmelderin haben gezeigt, daß es vorteilhaft ist, wenn ein Vergleich der Amplitudenwerte und ein Vergleich der Frequenz während einer Berechtigungsprüfung mittels eines ID-Codes innerhalb eines Authentifizierungsprozesses durchgeführt wird. Damit beansprucht das erfindungsgemäße Verfahren keine zusätzliche Zeit zum Erkennen einer Weiterleitung und läßt sich vorteilhaft bei Anwendungen im Bereich von Kraftfahrzeugen

35

einsetzen. Des Weiteren ist bei der Anwendung im KFZ-Bereich die Zeitspanne für den Authentifizierungsprozeß von 50 - 130 ms zu kurz, um mit vertretbarem Aufwand eine Entschlüsselung der Amplitudenwerte, die mit dem Antwortsignal zurückgesendet werden, durchzuführen, oder mittels eines anderweitigen Verfahrens die unterschiedlichen Dämpfungsscharakteristika von Hinweg und Rückweg auszugleichen. Damit kann eine unberechtigte Authentifizierung durch eine Weiterleitung zuverlässig ausgeschlossen werden.

Das erfindungsgemäße Verfahren soll nachfolgend anhand der Ausführungsbeispiele im Zusammenhang mit den Zeichnungen erläutert werden. Es zeigen, die

- Fig. 1 ein Ausführungsbeispiel der Erfindung als Verfahren zur Bestimmung der Amplitudendämpfung bei einer bidirektionalen Datenübertragung mit Weiterleitung, und  
Fig. 2 ein Ausführungsbeispiel der Erfindung als Verfahren zur Bestimmung der Amplitudendämpfung bei gleichzeitigem Vergleich der Trägerfrequenzen ohne Weiterleitung, und  
Fig. 3 ein Ablaufplan des Authentifizierungsprozesses in Zusammenhang mit dem in Figur 2 dargestellten Ausführungsbeispiels.

Die Aufgabe des in Figur 1 abgebildeten Ausführungsbeispiels ist es, während eines Datenaustausch zwischen einer ersten Sende- und Empfangseinheit und einer zweiten Sende- und Empfangseinheit mittels eines Vergleichs der Amplitudendämpfung zwischen dem Hinweg und dem Rückweg eine Weiterleitung zu erkennen. Eine derartige Anordnung läßt sich beispielsweise bei der Authentifizierung bei Systemen im KFZ-Bereich einsetzen, um eine Weiterleitung zu erkennen. Das dargestellte System besteht aus einer ersten Sende- und Empfangseinheit RXTX2, die im folgenden als Basisstation bezeichnet wird, einer zweiten Sende- und Empfangseinheit RTX1, die im folgenden als Transponder bezeichnet wird. Des weiteren ist ein Weiterleitungsgerät WL eingezeichnet das die Kommunikationsstrecke zwischen der Basisstation RXTX2 und dem Transponder RXTX1 verlängert. Die Kommunikationsstrecke von der Basisstation zum Transponder wird als UPLINK, die entgegengesetzte Kommunikationsstrecke als DOWNLINK bezeichnet. Im Folgenden wird der Aufbau der einzelnen Geräte erläutert.

Die Basisstation RXTX2 besteht aus einer Oszillatoreinheit OSC2, die eine Trägerfrequenz F2 zur Modulation für einen Ausgangsverstärker TX2 erzeugt. Mit den von einer Datenverarbeitungseinheit DP2 gelieferten Daten, erzeugt der Ausgangsverstärker TX2 ein moduliertes Ausgangssignal F2OUT, das mittels einer Sende- und Empfangsantenne AN2 als Fragesignal mit der Leistung P2OUT ausgesendet wird. Ferner ist die Sende- und Empfangsantenne AN2 mit einem Eingangsverstärker RX2 verbunden, um ein ankommendes Eingangssignal F2IN, das eine Eingangsleistung P2IN aufweist, verstärkt an einen Signalprozessor SP2

weiterzuleiten. Der Signalprozessor SP2 mißt die Höhe der Amplitude des Eingangssignals F2IN und leitet den gemessenen Wert A2 an die Datenverarbeitungseinheit DP2 weiter. Ferner demoduliert der Signalprozessor SP2 das Eingangssignal F2IN und leitet die aus dem Trägersignal gewonnenen Daten an die Datenverarbeitungseinheit DP2 weiter.

5 Zur Verlängerung der UPLINK-Kommunikationsstrecke durch das Weiterleitungsgerät WL, wird das von der Basisstation RXTX2 ausgesendete Fragesignal von einer ersten Empfangsantenne E1 an einen Verstärker RY1 weitergeleitet, der das um den Faktor G1 verstärkte Fragesignal mittels einer ersten Sendeantenne S1 wieder abstrahlt. Zur Verlängerung der DOWNLINK-Kommunikationsstrecke durch das Weiterleitungsgerät WL, wird ein von  
10 dem Transponder RXTX1 ausgesendetes Antwortsignal von einer zweiten Empfangsantenne E2 an einen zweiten Verstärker RY2 weitergeleitet, der das um den Faktor G2 verstärkte Antwortsignal durch eine zweite Sendeantenne S2 wieder aussendet.

Der Transponder RXTX1 besteht aus einer Oszillatoreinheit OSC1, die eine Trägerfrequenz F1 zur Modulation für einen Ausgangsverstärker TX1 erzeugt. Mit den von einer Datenverarbeitungseinheit DP1 gelieferten Daten, erzeugt der Ausgangsverstärker TX1 ein moduliertes  
15 Ausgangssignal F1OUT, das mittels einer Sende- und Empfangsantenne AN1 als Antwortsignal mit der Sendeleistung P1OUT ausgesendet wird. Ferner ist die Sende- und Empfangsantenne AN1 mit einem Eingangsverstärker RX1 verbunden, um ein ankommendes Eingangssignal F1IN, das eine Eingangsleistung P1IN aufweist, verstärkt an einen Signalprozessor SP1 weiterzuleiten. Der Signalprozessor SP1 mißt die Höhe der Amplitude des Ein-  
20 gangssignals F1IN und leitet den gemessenen Wert A1 an die Datenverarbeitungseinheit DP1 weiter. Ferner demoduliert der Signalprozessor SP1 das Eingangssignal F1IN und leitet die aus dem Trägersignal gewonnenen Daten an die Datenverarbeitungseinheit DP1 weiter.

25 Für den UPLINK wird die Größe der Dämpfung zwischen der Basisstation RXTX2 und dem Weiterleitungsgerät WL durch einen Kopplungsfaktor K21 und die Dämpfung zwischen Weiterleitungsgerät und Transponder durch einen Kopplungsfaktor K11 beschrieben. Entsprechend wird für den DOWNLINK die Dämpfung zwischen Transponder RXTX1 und Weiterleitungsgerät WL mit einem Kopplungsfaktor K12 und die Dämpfung mit einem Kopplungsfaktor K22 beschrieben. Ferner wird die Kopplung der Antennen E1 und S2 durch einen  
30 Faktor KRY21 und die Kopplung der Antennen S1 und E2 durch einen Faktor KRY12 beschrieben.

Im Folgenden wird die Funktionsweise erläutert. Im UPLINK wird durch das Weiterleitungs-  
35 gerät WL die Kommunikationsstrecke verlängert, indem das Weiterleitungsgerät WL ein von der Basisstation RXTX2 ausgesendetes Fragesignal empfängt und verstärkt wieder abstrahlt. Das Fragesignal wird von dem Transponder RXTX1 demoduliert und den gemessenen Wert der Amplitude A1 des Fragesignals als Datum in einem Antwortsignal für den DOWNLINK wieder zurückgesendet. Im DOWNLINK wird dann durch das Weiterleitungsge-



rät WL die Kommunikationsstrecke verlängert, in dem das empfangene Antwortsignal an die Basisstation RXTX2 verstärkt abgestrahlt wird. Die Basisstation RXTX2 demoduliert das empfangene Antwortsignal und vergleicht in der Datenverarbeitungseinheit DP2 der mit dem Antwortsignal zurückgesendete Wert der Amplitude A1 mit dem gemessenen Wert der Amplitude A2 des Antwortsignals. Sind die beiden Werte der gemessenen Amplituden unterschiedlich, wird von der Datenverarbeitungseinheit DP2 in einem internen Speicher die Zahl 1 abgelegt und eine Weiterleitung angezeigt. Liegt das Ergebnis des Vergleichs innerhalb eines vorgegebenen Intervalls, wird in dem Speicher die Zahl Null abgelegt und eine Weiterleitung ausgeschlossen.

Bei vorgegebener Sendeleistung P2OUT und P1OUT und bei vorgegebener Verstärkung der Eingangssignale P2IN und P1IN von Basisstation RXTX2 und Transponder RXTX1, sind die Werte A1 und A2 der Amplituden des Fragesignals und des Antwortsignals von den Kopplungsfaktoren für den UPLINK und den DOWNLINK sowie den Verstärkungsfaktoren G1 und G2 des Weiterleitungsgerätes WL abhängig. In dem vorliegenden Beispiel gilt für die Weiterleitung für die UPLINK ein Kopplungsfaktor KUL:

$$KUL = K21 + G1 + K11$$

und für den DOWNLINK ein Kopplungsfaktor KDL:

$$KDL = K12 + G2 + K22$$

Bedingt durch die Unsymmetrie des Übertragungsweges zwischen UPLINK und DOWNLINK, sind die beiden Kopplungsfaktoren KDL bzw. KUL und die Dämpfung der Amplituden A1 und A2 unterschiedlich. Im Unterschied dazu weist der Übertragungsweg eine symmetrische Dämpfungscharakteristik auf, wenn das Weiterleitungsgerät aus der Kommunikationsstrecke entfernt wird. Damit gilt dann für die beiden Kopplungsfaktoren von UPLINK und DOWNLINK KDL und KUL:

$$KDL = KUL$$

Ferner gilt für den Weiterleitungsfall, daß die Amplitudendämpfung durch die zusätzlichen Kopplungsfaktoren und der darin enthaltenen Freiraumdämpfung größer ist, als für den Fall in dem keine Weiterleitung stattfindet. Aus dem Unterschied der Dämpfungscharakteristik mit Weiterleitungsgerät WL und ohne Weiterleitungsgerät WL, ergibt sich für aus dem Vergleich der Amplituden A1 und A2 ein zuverlässiges Verfahren zum Erkennen einer Weiterleitung. Dies gilt auch dann, wenn das Weiterleitungsgerät WL versucht die Unsymmetrie der Dämpfungscharakteristik mittels der Verstärkung G1 und G2 auszugleichen, da dies ohne

Kenntnis der Kommunikationsentfernungen bzw. der Kopplungsfaktoren K11 bis K22 nicht mit einem vertretbaren Aufwand durchführbar ist. Sofern das Weiterleitungsgerät WL auf der Trägerfrequenz F1 eine Verstärkung der Amplituden A1 bzw. A2 durchführt, bestimmen die Kopplungsfaktoren KRY12 und KRY21 die maximal zulässige Verstärkung G1 bzw. G2. Um durch eine Rückkopplung ein Schwingen des Weiterleitungsgerät WL zu verhindern, muß die Kreisverstärkung des Weiterleitungsgerätes WL kleiner als 1 bleiben.

In dem weiteren Ausführungsbeispiel dargestellt in Figur 2 wird bei der Kommunikation zwischen der Basisstation RXTX2 und dem Transponder RXTX1 zusätzlich zu dem in Figur 1 bereits beschriebenen Vergleich der Amplituden auch ein Vergleich der Trägerfrequenzen des Fragesignals und des Antwortsignals durchgeführt. Entsprechend ist der im Folgenden beschriebene funktionale Aufbau der Basisstation RXTX2 und des Transponders RXTX1 bis auf die angeführten Erweiterungen mit dem der in Figur 1 dargestellten Funktionen identisch. Ferner findet in der dargestellten Ausführung die Kommunikation zwischen der Basisstation RXTX2 und des Transponders RXTX1 ohne eine Weiterleitung statt, weshalb der Kopplungsfaktor für den UPLINK KUL mit dem Kopplungsfaktor für den DOWNLINK KDL identisch ist. Eine bevorzugte Anwendung des Ausführungsbeispiels innerhalb eines Authentifizierungsprozesses wird in Zusammenhang mit den Ausführungen in Zusammenhang mit der Figur 3 erläutert.

Innerhalb der Basisstation RXTX2 wird das von dem Oszillator OSC2 erzeugte Trägersignal F2 zusätzlich einer Frequenzvergleichseinheit FC zugeführt, deren Ausgang mit der Datenverarbeitungseinheit DP2 verbunden ist. Ferner wird der Frequenzvergleichseinheit FC das durch den Empfangsverstärker RX2 verstärkte Antwortsignal, dessen Träger mittels einer Einheit CLK2 regeneriert wird, zugeführt. Im Transponder RXTX1 ist die Oszillatoreinheit OSC1 durch eine Einheit CLK1 ersetzt. Der Einheit CLK1 wird das von dem Eingangsverstärker RX1 verstärkte Fragesignal zur Regeneration des Trägers. Nach der Regeneration wird der Träger mit einer Frequenz F21 dem Ausgangsverstärker TX1 zur erneuten Modulation zugeführt und anschließend ausgesendet.

Im Folgenden wird die Funktionsweise erklärt. Mit dem Beginn des Aussendens des Fragesignals wird der Frequenzvergleichseinheit FC das unmodulierte Trägersignal F2 zugeführt. Sobald der Transponder RXTX1 das Fragesignal empfängt, wird durch eine Regeneration des Trägersignals mittels der Einheit CLK1 ein unmodulierter Träger mit der Frequenz F21 gewonnen und zur erneuten Modulation dem Sendeverstärker TX1 zugeführt, der das Antwortsignal an die Basisstation RXTX2 zurücksendet. Damit wird eine starre Frequenzkopplung durchgeführt. Sobald in der Basisstation RXTX2 das Antwortsignal empfangen wird, wird der von der Einheit CLK2 aus dem Antwortsignal gewonnene Träger mit der Frequenz F21 für einen Vergleich der Frequenzen von Fragesignal und Antwortsignal der Frequenz-

vergleichseinheit FC zugeführt. Damit liegt die Frequenz F2 der Oszillatoreinheit OSC2 und die Frequenz F21 aus dem Antwortsignal an der Einheit FC an. Sofern die beiden Frequenzen gleich sind, legt die Frequenzvergleichseinheit FC an die Datenverarbeitungseinheit DP2 ein Signal an. Ergibt die von der Datenverarbeitungseinheit DP2 gleichzeitig durchgeführte  
5 Auswertung der Amplituden, daß auch die beiden Werte der Amplituden A1 mit A2 gleich sind, wird eine Weiterleitung ausgeschlossen.

Der Ablauf eines Authentifizierungsprozesses auf der Grundlage des in Figur 2 dargestellten Ausführungsbeispiels wird in Figur 3 beschrieben.

10 Nach dem Start der Authentifikation, beispielsweise durch Betätigen des Türgriffs am Fahrzeug, sendet der Ausgangsverstärker TX2 der Basisstation RXTX2 in einem ersten Prozessschritt SENDEN SN2 ein Fragesignal SN2, das vorzugsweise verschlüsselte Daten enthält. In einem nachfolgenden Prozessschritt EMPFANG SN2 wird das Fragesignal von dem Ein-  
15 gangsverstärker RX1 in dem Transponder RXTX1 verstärkt und anschließend weitergeleitet. Während die Einheit CLK1 in einem Prozessschritt F2 EXTRAKTION den Träger aus dem Fragesignal zurückgewinnt, wird in den parallel ablaufenden Prozessschritten AM1 MESSEN und DATA EXTRAKTION innerhalb der Signalprozessoreinheit SP1 der Wert der Amplitude A1 gemessen und die Daten vom Träger abgetrennt. In einem folgenden Prozessschritt DA-  
20 TA DECRYPT werden die Daten entschlüsselt und in einem Frageschritt ID-CODE die Übereinstimmung mit einem internen gespeicherten Code überprüft. Ist der ID-Code ungültig, wird der Authentifizierungsprozeß beendet und es wird kein Antwortsignal zurückgesendet, ist der ID-Code gültig, wird der gemessene Wert der Amplitude A1 in einem nachfolgenden Prozessschritt ENCRYPT verschlüsselt und in einem darauffolgenden Prozessschritt SENDEN  
25 SN1 vom Ausgangsverstärker TX1 als Antwortsignal zurückgesendet. Nach dem Empfang des Antwortsignals in der Basisstation RXTX2, gekennzeichnet durch den Prozessschritt EMPFANG SN1, wird, während in einem Prozessschritt F21 EXTRAKTION die Einheit CLK2 für den Frequenzvergleich den Träger regeneriert, gleichzeitig in den parallel ablaufenden Prozessschritten AM2 MESSEN und DATA EXTRAKTION innerhalb der Signalprozessorein-  
30 heit SP2 der Wert der Amplitude A2 gemessen und die Daten vom Träger abgetrennt. In einem folgenden Prozessschritt DATA DECRYPT werden die Daten entschlüsselt und in einem Frageschritt ID-CODE die Übereinstimmung des zurückgesendeten ID-Codes mit einem internen gespeicherten Code überprüft. Ist der ID-Code ungültig, wird der Authentifizierungs-  
35 prozeß beendet, ist der ID-Code gültig, wird in zwei nachfolgenden Frageschritten F? und A? die Frequenz F2 auf Übereinstimmung mit der Frequenz F21 und das Verhältnis der Amplituden A1 und A2 auf Übereinstimmung mit einem vorgegebenen Wert überprüft. Wird eine der Abfragen verneint, wird der Authentifizierungsprozeß beendet. Werden beide Abfragen bejaht, wird der Authentifizierungsprozeß erfolgreich abgeschlossen, d.h. es wird in einem nachfolgenden Prozessschritt UNLOCK die Türe des Fahrzeugs entriegelt.

Heilbronn, den 12.02.2001  
FTP/H-dk/dk – P303515

Patentansprüche

5

1. Verfahren zur Erkennung einer Weiterleitung bei einer bidirektionalen kontaktlosen Datenübertragung zwischen einer ersten Sende- und Empfangseinheit (RXTX2) und einer zweiten Sende- und Empfangseinheit (RXTX1),

**dadurch gekennzeichnet, daß**

- 10
- die erste Sende- und Empfangseinheit (RXTX2) ein Fragesignal ausgesendet,
  - von der zweiten Sende- und Empfangseinheit (RXTX1) den Wert der Amplitude (A1) des empfangenen Fragesignal gemessen wird,
  - der gemessene Wert der Amplitude (A1) in einem Antwortsignal zurücksendet wird,
  - von der ersten Sende- und Empfangseinheit (RXTX2) der Wert der Amplitude (A2) des empfangenen Antwortsignals gemessen und mit dem zurückgesendeten Wert der Amplitude (A1) verglichen wird.
- 15

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, daß** in Abhängigkeit des Ergebnisses des Vergleichs einer Weiterleitungsanzeige ein vorbestimmter Wert zugewiesen wird.
- 20

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, daß** der gemessene Wert (A1) der Amplitude in verschlüsselter Form mit dem Antwortsignal übertragen wird.

- 25
4. Verfahren nach Anspruch 3, **dadurch gekennzeichnet, daß** der Vergleich innerhalb eines vorgegebenen Zeitfensters durchgeführt wird, das mit dem Beginn des Aussenden des Fragesignals beginnt.

- 30
5. Verfahren nach einem der vorangegangenen Ansprüchen, **dadurch gekennzeichnet, daß** die erste Sende- und Empfangseinheit (RXTX2) zusätzlich die Frequenz (F2) des Fragesignals mit der Frequenz (F21) des Antwortsignals vergleicht.

- 35
6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, daß** von der ersten Sende- und Empfangseinheit (RXTX2) geprüft wird, ob die Trägerfrequenz mit dem Aussenden des Fragesignals bis zum Empfang des Antwortsignals ohne Unterbrechung anliegt.

7. Verfahren nach einem der vorangegangenen Ansprüche, **dadurch gekennzeichnet, daß** der Vergleich der Amplitudenwerte ( $A_1$ ,  $A_2$ ) und der Vergleich der Frequenzen ( $F_2$ ,  $F_{21}$ ) gleichzeitig mit einer Überprüfung eines Identifikationscodes durchgeführt wird.
- 5 8. Verwendung des Verfahrens nach einem der vorangegangenen Ansprüche zur Erkennung einer unberechtigten Weiterleitung eines Authentifizierungsprozesses bei Kraftfahrzeugen.

Heilbronn, den 12.02.2001  
FTP/H-dk/dk – P303515

5

### **Zusammenfassung**

1. Verfahren zur Erkennung einer Weiterleitung bei einer bidirektionalen, kontaktlosen Datenübertragung.

10

- 2.1 Bei den bisher bekannten Verfahren zur bidirektionalen, kontaktlosen Datenübertragung läßt sich durch eine Weiterleitung der Kommunikation mittels Funkverstärkern die Kommunikation derart manipulieren, daß sich Unberechtigte authentifizieren können.

15

- 2.2 Mit dem neuen Verfahren wird eine unberechtigte Authentifizierung verhindert, indem bei einer bidirektionalen, kontaktlosen Datenübertragung die Dämpfung der Amplitude von dem Hinweg mit der Dämpfung der Amplitude von dem Rückweg verglichen wird. Sind die ermittelten Dämpfungswerte gleich groß, kann eine Weiterleitung ausgeschlossen werden. Um die Sicherheit zusätzlich zu erhöhen, kann außerdem ein die Trägerfrequenz des Fragesignals mit der Trägerfrequenz des Antwortsignals verglichen werden.

20

1/3

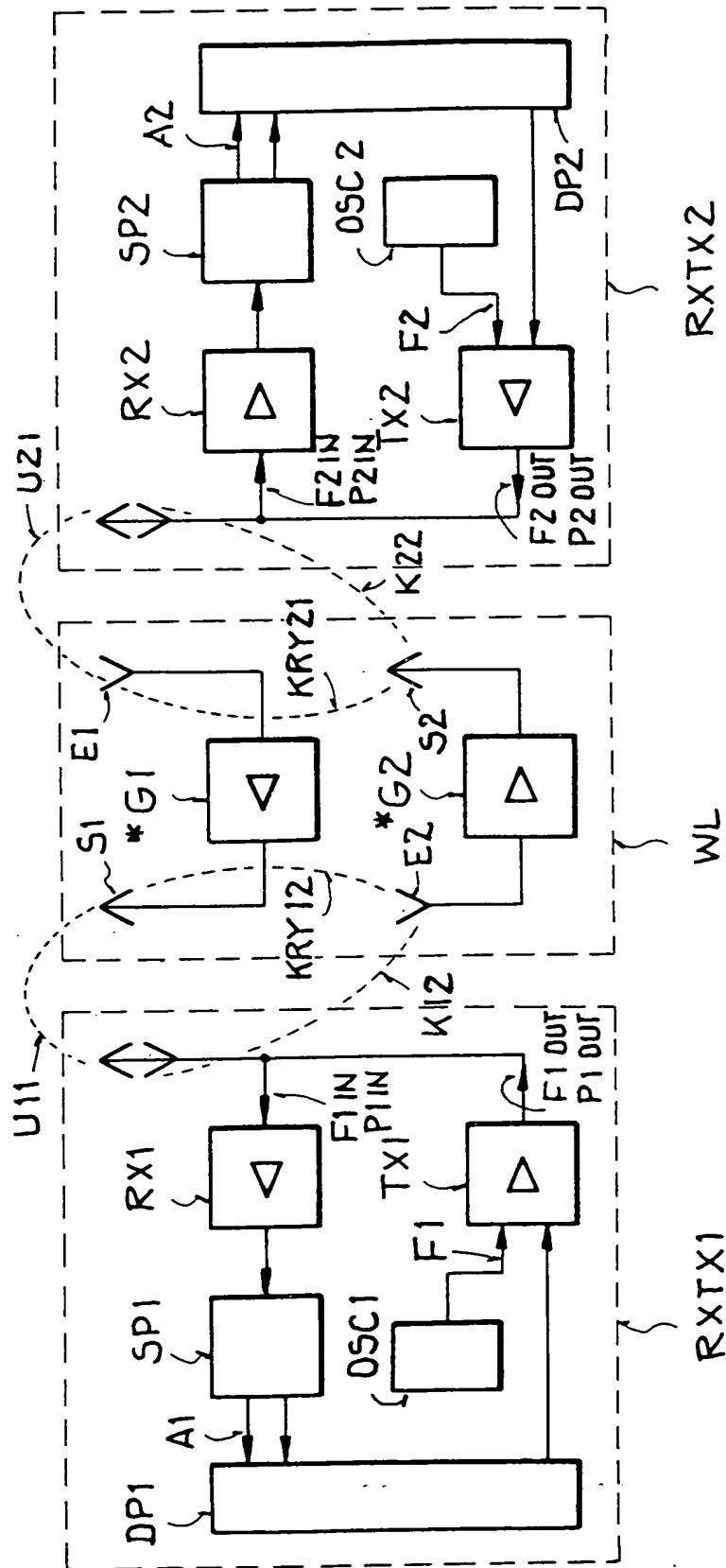


FIG.1

2/3

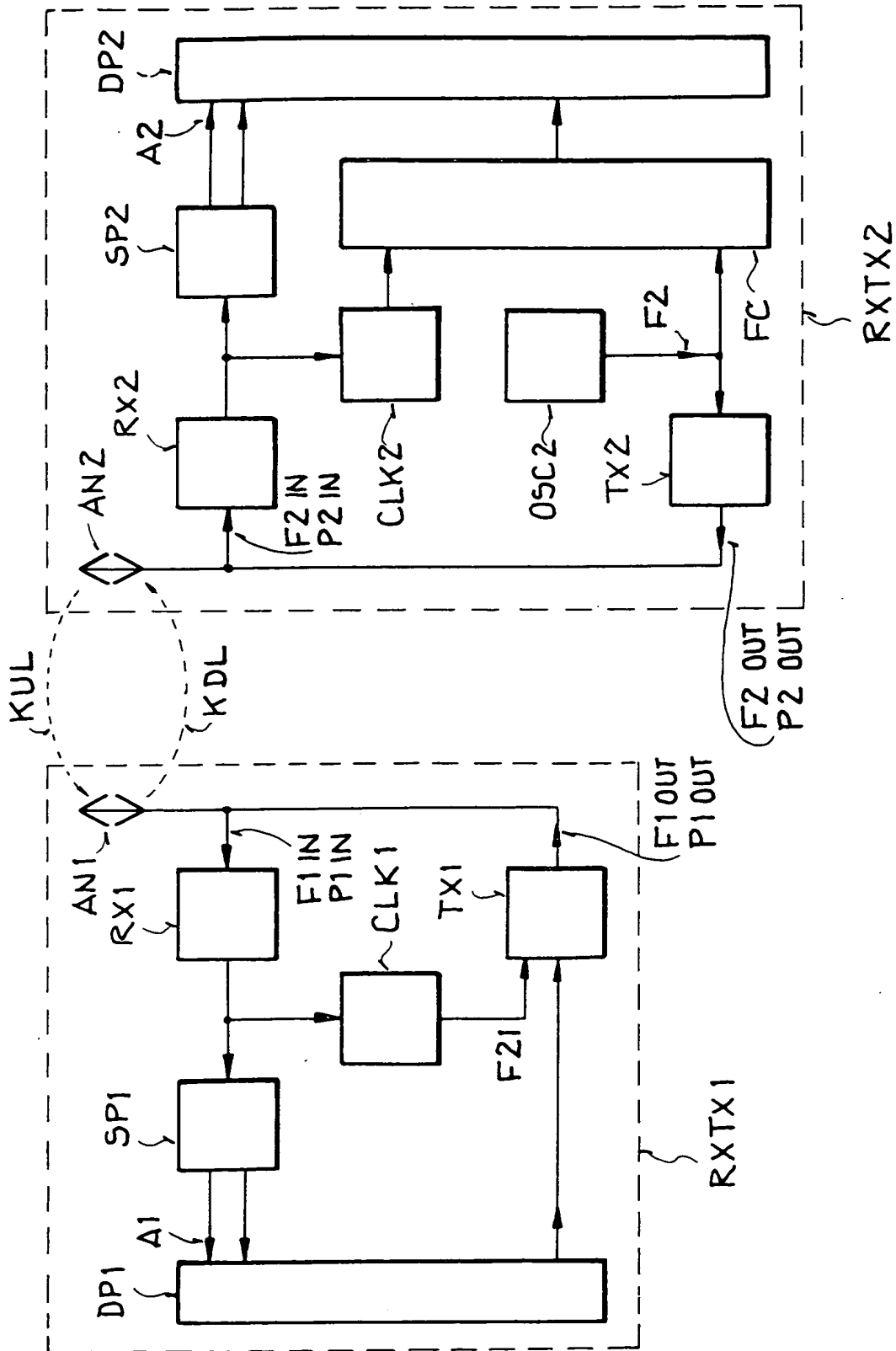


FIG. 2



3/3

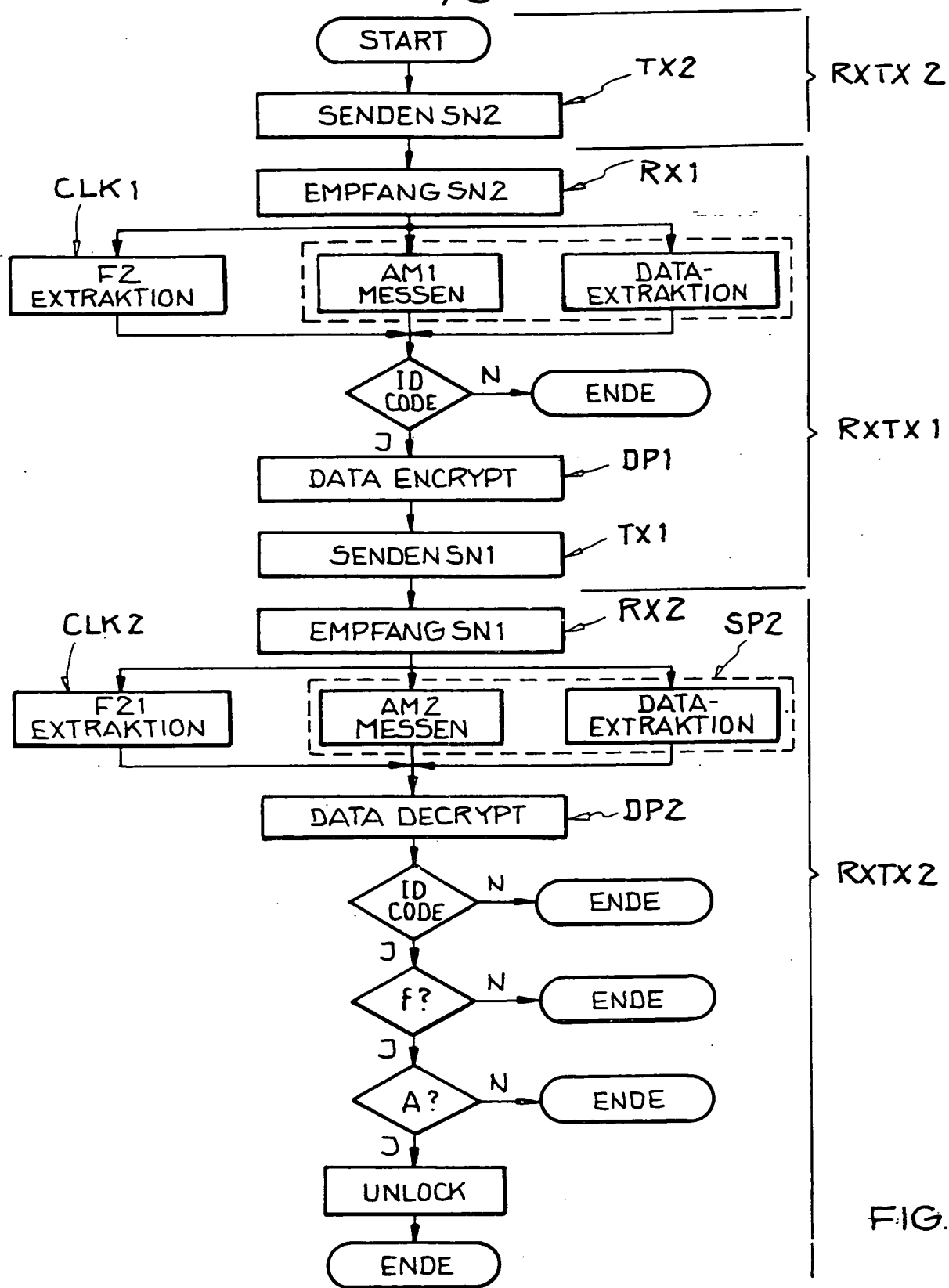


FIG.3